Annual 47 CFR § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for [*Insert year*] covering the prior calendar year [*Insert year*]

1. Date filed: 2/2/2018

2. Name of company(s) covered by this certification: Radio Commuications of Charleston, Inc.

3. Form 499 Filer ID: 819718

4. Name of signatory: R. Buckner

5. Title of signatory: President

6. Certification:

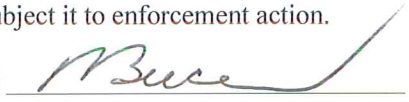
I, R. Buckner, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, record-keeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company *has not* taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, provide an explanation of any actions taken against data brokers.]

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI. [NOTE: If you reply in the affirmative, provide a summary of such complaints. This summary must include the number of complaints, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed  President, Radio Comm. of Charleston, Inc.

Attachments: Accompanying Statement explaining CPNI procedures

Policy Name: Customer Private Network Information Policy/Identity Theft Prevention Program
Composed by: Rick Buckner, CEO
Effective date: 12 Jan 2006

Safeguarding CPNI ~ We will take reasonable measures to discover and protect against attempts of unauthorized customers to gain access to Customer Proprietary Network Information (CPNI). During the customer's phone or in-store visit process, we will use authentication to insure we are communicating with the customer account owner.

We will only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides us with an authentication password.

Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords ~ To establish a password, we will authenticate the customer without the use of readily available biographical information, or account information. We will create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

Telephone access to CPNI ~ We will only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the us with a password, as described above, that is not prompted by us asking for readily available biographical information, or account information. If the customer does not provide a password, then we will only disclose call detail information by sending it to the customer's address of record, or, by calling the customer at the telephone number of record. If the customer is able to provide us with call detail information a customer-initiated call without assistance, then we are permitted to discuss the call detail information provided by the customer.

We will not have online access to CPNI account information.

In-store Access to CPNI ~ In-store access to CPNI will only be disclosed if the customer validates their identity by providing a valid photo ID matching the customer's account information.

Password Back-up Authentication ~ We will use a Password and Back-up Authentication method for lost and forgotten Passwords. We will authenticate the customer without the use of readily available biographical information, or account information. We will create a back-up customer authentication method in the event of lost or forgotten passwords, but such back-up customer authentication method may not

prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described above.

Non-Cash Payments ~ A second form of ID is required to process a credit card or check payment to validate identity of purchaser. Your initials must be on the check or the credit card receipt to indicate that the information was validated and authorized by your supervisor. For credit card payments over the phone – a Credit Card Authorization form must accompany the credit card receipt.

Training ~ Mandatory training will be done on a semi-annual basis. This training will include, but not be limited to - review of this policy; review of any updates on CPNI/Identity Theft rules and regulations; review of any updates regarding new risks and vulnerabilities. Validation of this training will be kept in personnel records.

Notification ~ We will notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be provided through a voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

Specific Action ~ In accordance with the CPNI requirements, RCC must have a policy that delineates specific action to be taken upon violation of the CPNI policy. In that regard, RCC will specifically address and investigate violations and the root causes of those violations of our CPNI policy and suspend without pay or terminate employment of offenders of the policy.

If identity theft (red flag) is suspected, it must be brought to the General Manager's attention immediately. The General Manager will assess the situation and customize a plan of action for the red flag.

We shall notify law enforcement of a breach of our customers' CPNI as provided in this procedure. We shall not notify our customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until we have completed the process of notifying law enforcement pursuant to the above procedure.

As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of a breach, we shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni.

We will adhere to the following Federal Communications Commission FCC 07-2253 as follows:

(1) Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (2) and (3).

(2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (1), in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

(a) Customer Notification. After a telecommunications carrier has completed the process of notifying law enforcement pursuant to paragraph (1), it shall notify its customers of a breach of those customers' CPNI.

(b) Recordkeeping. All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (1), and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.

(c) Definitions. As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

(d) This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

Employee Acknowledgement ~

I understand the importance of the CPNI Policy and agree to comply with the policy.

Name **Date**

External Company Agreement to comply with the CPNI policy of Radio Communications of Charleston, Inc.

To Whom it May Concern:

We agree to comply with attached Radio Communications of Charleston, Inc, written company policy while accessing proprietary CPNI company data and when CPNI data is in our possession. Specifically, this means that we will exercise all caution and protective measures possible to protect the company's CPNI information. Furthermore, during the periods of data access and when the information is in our possession we will assume all liability related to the loss, unauthorized dissemination, or otherwise inappropriate distribution or unauthorized use of this information in accordance with the CPNI regulations of the Federal Communications Commission, specifically as stated in this policy.

_____

Agreed ~ (any external company with access)

_____

Date